Progress Has Been Made in Protecting Critical Assets

February 2003

Reference Number: 2003-20-047

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

February 10, 2003

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION &
CHIEF INFORMATION OFFICER

Gordon C. Milbourn III

FROM: Gordon C. Milbourn III
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Progress Has Been Made in Protecting Critical Assets (Audit # 200220027)

This report presents the results of our review of the Internal Revenue Service's (IRS) actions to protect its critical infrastructure. The overall objective of this review was to determine whether the IRS had effectively implemented its plan for protecting its critical cyber-based infrastructure. We conducted this review in conjunction with other similar audits performed by members of the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency.

The Policy on Critical Infrastructure Protection: Presidential Decision Directive (PDD) 63, dated May 1998, calls for a national effort to assure the security of the nation's critical infrastructure. The infrastructure includes systems essential to the minimum operations of the economy and government, such as telecommunications, banking and finance, energy, and transportation. The PDD 63 requires that each government department and agency prepare a plan for protecting its own critical infrastructure.

The current Administration has issued two Executive Orders (EO) relating to the protection of the nation's critical infrastructure. *Executive Order Establishing the Office of Homeland Security and the Homeland Security Council* (EO 13228), issued October 8, 2001, provides for coordination of efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks. *Critical Infrastructure Protection in the Information Age* (EO 13231), issued October 16, 2001, established a Critical Infrastructure Protection Board.

In summary, the IRS has not yet completed its Critical Infrastructure Protection Plan, but it has identified its critical cyber assets and has taken significant steps to protect them.

Although some areas need improvement, the IRS has recognized them and has adequate plans in place to address the issues. These issues include: completing risk mitigation activities, implementing the Business Continuity Plan, protecting the infrastructure, obtaining the necessary training for key security employees, and improving security awareness for all employees with access to critical systems.

Two other areas, however, have not been adequately addressed. First, the IRS has not coordinated with the over 250 federal and state agencies for which it provides data to determine the impact if those data could not be obtained during an emergency, and has not determined the value of information received from many federal and state agencies. With the sharing of information in today's government, an emergency in one agency could have a significant impact on many other agencies. Second, the IRS has not determined the resources needed to protect its critical assets. As a result, it has no assurance that all key positions are filled and whether additional funding is needed to acquire those resources.

We recommended the Chief Infrastructure Assurance Officer (CIAO) take actions to coordinate with those agencies receiving information from or providing information to the IRS to ensure that critical data are identified and protected. The CIAO should also identify the resources needed to protect the IRS' critical assets, evaluate the impact of diverting resources from other important assets in an emergency, and ask for funding if needed to fill any gaps.

Management's Response: The Chief, Security Services, concurred with our recommendations and stated the IRS will take action to determine the appropriate level of security needed to adequately protect all critical data, whether shared or received. Also, management has reviewed its resource requirements and is satisfied that resources are adequate to protect its critical infrastructure and mission critical assets. Management's complete response to the draft report is included as Appendix IV.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Gary V. Hinkle, Acting Assistant Inspector General for Audit (Information Systems Programs), at (202) 927-7291.

Table of Contents

Background

The Policy on Critical Infrastructure Protection: Presidential Decision Directive (PDD) 63, dated May 22, 1998, calls for a national effort to assure the security of the nation's critical infrastructure. This infrastructure consists of physical and cyber-based systems essential to the minimum operations of the economy and government. It includes, but is not limited to, telecommunications, banking and finance, energy, transportation, and essential government services.

The current Administration has issued two Executive Orders (EO) designed to improve the Federal Government's critical infrastructure program in the context of the PDD 63. *Executive Order Establishing the Office of Homeland Security and the Homeland Security Council* (EO 13228), issued October 8, 2001, provides for coordination of efforts to protect the United States and its critical infrastructure from the consequences of terrorist attacks. *Critical Infrastructure Protection in the Information Age* (EO 13231), issued October 16, 2001, established a Critical Infrastructure Protection Board.

The PDD 63 requires that each government department and agency prepare a Critical Infrastructure Protection Plan (CIPP) for protecting its own critical infrastructure, including, but not limited to, its cyber-based systems.

The President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency initiated a review of the nation's critical infrastructure assurance program in 1999. To support this, government-wide audits are being conducted by the agencies' Offices of Inspector General and consist of four phases. Phases I and II relate to critical cyber-based infrastructures, and Phases III and IV relate to critical physical infrastructures.

In our first report entitled, *The Internal Revenue Service Should Improve Actions to Protect Its Critical Infrastructure* (Reference Number 2000-20-097, dated June 2000), we evaluated the adequacy of the IRS' planning and assessment activities for protecting its critical cyber-based infrastructure.

In our second report entitled, *Efforts to Protect Critical Infrastructure Facilities Are Adequate* (Reference

Number 2001-20-111, dated July 2001), we evaluated the adequacy of the IRS' planning and assessment activities for protecting its critical physical infrastructures.

In this report, we are providing the results of our review of the IRS' implementation activities for protecting its critical cyber-based infrastructures.

The audit was conducted at the IRS' National Headquarters and in New York at the office of the Acting Deputy Director, Cyber Security, from August to November 2002. The audit was conducted in accordance with *Government Auditing Standards.* Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

The Internal Revenue Service Has Made Progress in Protecting Its Critical Assets

The IRS has identified 19 critical assets,[1] 12 critical business processes (e.g., processing refunds, processing tax returns), and 6 critical administrative processes (e.g., providing computing and communications resources, providing procurement services) as required by federal guidelines.

A CIPP covering these critical assets has been drafted but has not yet been formally approved by the IRS or the Department of the Treasury, and no target implementation date has been set.

Although the plan has not been formally approved, the IRS has taken significant actions to protect its critical assets. However, additional actions need to be taken. As the Federal Government's primary revenue collector, the IRS accounts for over $2 trillion in revenue annually. If the critical assets are not protected, government operations could be compromised. For example, an emergency during the filing season[2] could have a negative effect on the economy if tax refunds cannot be processed. Also, the IRS

[1] The IRS has identified critical assets (including buildings and computer systems) as called for in the PDD 63. Subsequently, the National Critical Infrastructure Assurance Officer identified six of these critical assets that may require priority attention from a security perspective.

[2] The filing season is the period from January through mid-April when most individual income tax returns are filed.

maintains financial data for over 130 million taxpayers. Unauthorized access to these data could negatively impact taxpayer confidence in the nation's tax system.

The following is our assessment of progress made for each of the following subject areas required to be addressed in a CIPP:

- Risk mitigation.
- Business Continuity Program.
- Interagency coordination.
- Infrastructure requirements.
- Resource requirements.
- People and skills requirements.
- Employee awareness program.

The IRS has made substantial progress to mitigate risks

The IRS took significant actions after September 11, 2001, to protect its employees from the threat of terrorism. It assessed and enhanced physical security at critical sites, improved mail handling procedures, increased its efforts to plan for disaster recovery, and established a high-level executive steering committee to manage emerging security risks.

The IRS has also made significant improvements to protect the vast amounts of sensitive data it is charged with protecting. For example, mainframe operating system security controls are generally adequate. In addition, virus protection has improved, intrusion detection systems are being installed, and networks are being standardized.

However, the Office of Management and Budget (OMB) and the Department of the Treasury guidelines require that the presence of adequate security controls must be certified before a system is implemented and at least every 3 years thereafter. To date, 4 of 15 critical applications have been certified, and the IRS expects to certify 14 of those 15 critical applications by April 2003. The remaining application will not be certified because it is being replaced during the IRS' modernization efforts.

We were advised that delays in system certifications were due primarily to new technology migration from one platform to another, new tax law updates which result in changes in system functionality and structural system changes, system consolidations, process improvements, new system interfaces, data relocation, and database redesign.

The IRS has made substantial progress in developing and implementing its Business Continuity Program

The IRS has made substantial progress in developing and implementing its Business Continuity Program that includes disaster recovery, business resumption, and other related efforts to ensure that IRS operations continue after experiencing a serious business interruption. The Security Executive Steering Committee oversees the IRS' Business Continuity Program. The IRS has:

- Developed disaster recovery plans for the computing centers and business resumption and disaster recovery plans for the IRS campuses. These plans are periodically tested and updated.
- Obtained emergency funding from the OMB after the September 11, 2001, disaster.
- Initiated plans to improve the recovery capability of its mainframe computers located at the computing centers. The IRS estimated it would take approximately 4 weeks to restore critical systems and 3 months to fully integrate and return supporting systems to operational levels that existed prior to a disaster.[3]
- Developed a continuity of operations plan for the IRS' National Headquarters, established offsite Situation Awareness and Management Centers (SAMC) for management's use during an emergency, and conducted a test of the continuity of operations plan using one of the SAMCs.

[3] For additional information, see "IRS-Wide Business Continuity Planning, Case For Action," Draft, dated November 30, 2001.

- Increased the visibility and management oversight of business continuity issues, for example, by identifying Master File[4] recovery as a material weakness under government financial reporting requirements.[5]
- Updated business continuity procedures in the Internal Revenue Manual (IRM).

However, in large IRS offices where more than one Business Unit is present, it is not clear whether each executive is responsible for developing individual Business Continuity Plans or whether one executive is responsible for developing these plans in each geographic location. The IRS has not clearly defined the functional duties, responsibilities, and reporting relationships of the Business Continuity Program in sufficient detail.

While the IRM assigns responsibilities for business continuity to "Heads of Offices," the IRS has not fully determined the executives to whom this applies. Without fully defining and assigning the business continuity duties, responsibilities, and job titles involved, the IRS may not be able to restore mission essential functions (e.g., collecting and depositing taxes) within a reasonable period of time. The inability to restore IRS operations could have a direct impact on government revenues.

We previously reported this condition, and the IRS responded that corrective actions would be taken by March 2003.[6]

The IRS has not coordinated with other agencies to ensure shared critical data is protected

The draft CIPP provides that the Critical Infrastructure Assurance Officer (CIAO) and the Critical Infrastructure Protection Management Officer are responsible for

[4] The Master File is the IRS' main computer system, consisting of taxpayer accounts.

[5] A material weakness is a control deficiency that the agency determines to be significant enough to be reported outside the agency (see Federal Managers' Financial Integrity Act of 1982, 31 U.S.C. §§ 1105, 1113, and 3512 (1994 & Supp. IV 1998)).

[6] *The Internal Revenue Service Has Made Substantial Progress in Its Business Continuity Program But Continued Efforts Are Needed* (Reference Number 2003-20-026, dated December 2002).

maintaining relationships and coordinating with other critical infrastructure protection organizations in industry and in foreign, federal, state, and local governments. However, the IRS' CIPP only assigns responsibility; it does not describe the purpose and procedures for the interagency coordination.

In another report currently issued in draft for the IRS' response, entitled, *Computer Security Weaknesses at State Agencies Put Federal Tax Information at Risk* (Audit Number 200220024), we detail that the IRS provides data to approximately 250 state and federal agencies. For example, data are provided to federal agencies such as the Social Security Administration and Health and Human Services, as well as state tax, welfare, and child care agencies.

The IRS has not determined the criticality of the support its assets provide to the missions of other agencies, nor has it determined the value of the information technology (IT) support received from other agencies.

The inability to obtain or provide critical data could have a detrimental effect on other agencies, not just the IRS. The IRS has not made interagency coordination a priority in the development of its infrastructure protection plans.

The IRS has begun to implement its plan for satisfying infrastructure requirements

The IRS has begun to improve Internet security. We have previously reported that the IRS had at least 24 Internet gateways, making it difficult to manage its cyber perimeter.[7] We recommended that the IRS reduce the number of gateways to a more manageable level to reduce costs and move toward more consistent security settings. To date, a standard configuration has not been established for Internet gateways. The IRS responded that corrective actions would be completed by late 2002.

[7] *Controls Over the Internet Gateway Should Be Improved to Better Deter and Detect External Attacks* (Reference Number 2001-20-101, dated June 2001).

The IRS has begun installing Intrusion Detection Systems (IDS) at its Internet gateways.[8] IDS sensors have been placed at external connection points to capture questionable traffic. This information is fed into a central point for analysis. The recently-created Computer Security Incident Response Capability (CSIRC) team monitors for potential incidents 24 hours a day and enters them into the incident database for follow-up. Qualified contractors are being used as necessary to assist in this effort.

The IRS is participating in a White House effort based on information sharing across the government. The goal is for incident response teams to share analytical techniques, tools, and intelligence information. Also participating in this effort are the Veterans Administration, Department of Defense, Department of Energy, and the Federal Aviation Administration.

This effort is designed to directly improve the IRS' security posture and that of the government sector by providing a vehicle for early warnings of cyber attacks. It will also provide for "fast-tracking" the adoption of security technologies based on what other agencies have deployed by permitting the IRS to quickly determine if a solution is viable within its environment. This effort is in the early stages, with initial tasks still being assigned.

We were advised that during the next 3 months, the IRS would connect to the Cyber Warning Information Network for early warnings that was established by the White House. This Network will be connected to the various Information Sharing and Analysis Centers in the private sector and several government agencies.

The data contained on IRS systems is extremely sensitive and needs to be protected. The systems the IRS has designated as critical can be used to access over 130 million taxpayer accounts. However, the IRS does not routinely review activity logs (audit trails) for these systems to identify unauthorized accesses, except for the Integrated Data Retrieval System (IDRS), which is the IRS' primary

[8] *Continued Emphasis Is Needed to Establish a Mature Intrusion Detection System* (Reference Number 2003-20-003, dated October 2002) (Limited Official Use).

system for accessing taxpayer account information. Malicious acts by employees and hackers pose as great a risk for the other critical systems and data as for the IDRS; thus, it is equally important that the IRS monitor activity on those systems. We previously reported this condition, and the IRS responded that corrective actions would be taken by December 2004.[9]

<u>The IRS has not identified its resource requirements</u>

The draft CIPP requires the identification of resource requirements (IT security personnel) for protecting critical infrastructure. The IRS is confident that it has sufficient resources to support critical assets in an emergency. However, diverting personnel to critical assets could impact assets that are non-critical but still important. The IRS has not identified its resource requirements and, therefore, actions cannot be taken to address any shortages that may exist. The Modernization, Information Technology & Security Services (MITS) organization had not, at the time of our review, taken the lead in identifying these requirements or assessing training needs. Until these processes are properly directed and controlled, important assets could be in jeopardy.

<u>The IRS has not been able to meet its people and skills requirements for IT security</u>

IRS employees with key security responsibilities are dispersed in many locations throughout the organization. Many report to the Deputy Commissioner for Modernization & Chief Information Officer, but others report to functional managers. Ensuring that each of these employees receives the appropriate training for his or her role is a difficult challenge.

The responsibility for recruitment, education, and awareness is assigned to the manager responsible for each critical asset. However, the CIPP does not include specific procedures to assist the owners in implementing these programs. The critical asset owners are responsible for determining whether necessary skill sets are identified and

[9] *User Activity on Most Sensitive Computer Systems Is Not Monitored* (Reference Number 2002-20-075, dated March 2002).

available to support critical infrastructure protection activities, but responsibility for determining the required training for skill sets is still uncertain. Although we believe it should, the MITS organization does not participate in assessing training needs.[10]

The National Institute of Standards and Technology (NIST) and the General Accounting Office (GAO) recommend that:

- Computer security training should be role-based. Role-based learning focuses on the job functions employees perform rather than on their job titles. It provides security training that satisfies the specific requirements of an employee's role.
- A system should be in place for effectively tracking each employee's training.
- Methods should be employed for determining whether employees have learned and retained what they have been taught, and whether their performance has improved.

Currently, IRS computer security training does not follow all NIST and GAO recommendations. Curricula for key security roles have not been developed. Although a system is available to track employees' training, it is not reliable. Also, testing and other follow-up techniques are not used to determine whether training was successful. As a result, the IRS cannot be sure that employees are adequately skilled to perform computer security duties, which could place critical systems at unnecessary risk.

We also previously reported this issue. The IRS responded that corrective actions would be taken by April 2004.[11]

[10] *Many Advances Made, But Additional Emphasis Is Needed on Key Initiatives in the Security Services Organization* (Reference Number 2003-20-005, dated October 2002).

[11] *Many Advances Made, But Additional Emphasis Is Needed on Key Initiatives in the Security Services Organization* (Reference Number 2003-20-005, dated October 2002).

The IRS has not implemented an adequate employee awareness program

The NIST and the GAO recommend that computer security awareness activities include the use of videotapes, newsletters, posters, new employee awareness training, and the signing of statements acknowledging the rules in effect. In order to measure the effectiveness of these awareness activities, they recommend:

- Using test measures, such as true/false or multiple-choice questions, to ascertain what has been learned and retained.
- Using incident reports to monitor for noncompliance with computer security.
- Observing how well employees follow recommended security procedures.
- Conducting periodic tests by contacting employees directly to measure their security awareness.

Security Services has provided a wide variety of computer security awareness activities using various methods and techniques as recommended by the NIST and the GAO. However, it does not have assurance that its efforts are having a positive effect. Security Services does not have a systematic method for regularly obtaining information or data on the impact of its computer security awareness activities. Such information could be used to evaluate the effectiveness of these activities, help measure trends in whether employee computer security awareness is improving or decreasing, and help redirect computer security awareness activities to the topics and audiences that need the most attention.

We consider employee awareness of security risks to be the IRS' weakest link in protecting taxpayer data and assets from disclosure or loss. In prior reports, we noted that even after the 2001 anthrax attacks, employees voluntarily opened mail at their desks or cubicles and not in the central mailroom as required.[12] In some cases, employees opened mail in public walk-in areas, and mail handlers did not x-ray all incoming mail. In another report,[13] we discussed that 71 of 100 employees we contacted were willing to change their password to one provided by a caller pretending to work on the Help Desk.

Recommendations

In prior reports, we have already made recommendations to address most of the issues cited above. In addition to those, we recommend the CIAO:

1. Identify the critical data that are shared with other federal and state entities and implement specific procedures to protect those data. Also, the CIAO should identify the critical data that are received by the IRS and implement specific procedures to protect those data.

Management's Response: Management agreed with our recommendation and stated the IRS will take action to determine the appropriate level of security needed to adequately protect all critical data, whether shared or received.

2. Identify resource requirements needed to protect the critical infrastructure, evaluate the impact of diverting personnel from protecting other assets in an emergency, and ask for funding if needed to fill any gaps.

Management's Response: Management agreed with our recommendation and has determined that resources are adequate to protect its critical infrastructure. Subsequent to the response, management advised that, in an emergency,

[12] *Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail* (Reference Number 2003-20-004, dated October 2002).
[13] *Management Advisory Report: Network Penetration Study of Internal Revenue Service Systems* (Reference Number 2002-20-057, dated March 2002).

sufficient resources should still exist to protect critical infrastructure and mission critical assets.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the Internal Revenue Service (IRS) had effectively implemented its plan for protecting its critical cyber-based infrastructure.

To determine whether the IRS' Critical Infrastructure Protection Plan (CIPP) had been effectively implemented, we discussed the status of the CIPP with responsible management officials and reviewed the draft CIPP to determine whether it contained adequate procedures.

We reviewed key documents, including the CIPP Asset Background Data, Business Continuity Process Mapping information, Internal Revenue Manual and Business Continuity web site references, and prior Treasury Inspector General for Tax Administration reports for each of the following areas:

- Risk mitigation.
- Business Continuity Program.
- Interagency coordination.
- Infrastructure requirements.
- Resource requirements.
- People and skills requirements.
- Employee awareness program.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)
Gary V. Hinkle, Acting Assistant Inspector General for Audit (Information Systems Programs)
Steve Mullins, Director
Gerald Horn, Audit Manager
Dan Ardeleano, Senior Auditor
Bret Hunter, Senior Auditor
William Lessa, Senior Auditor
David Hodge, Auditor

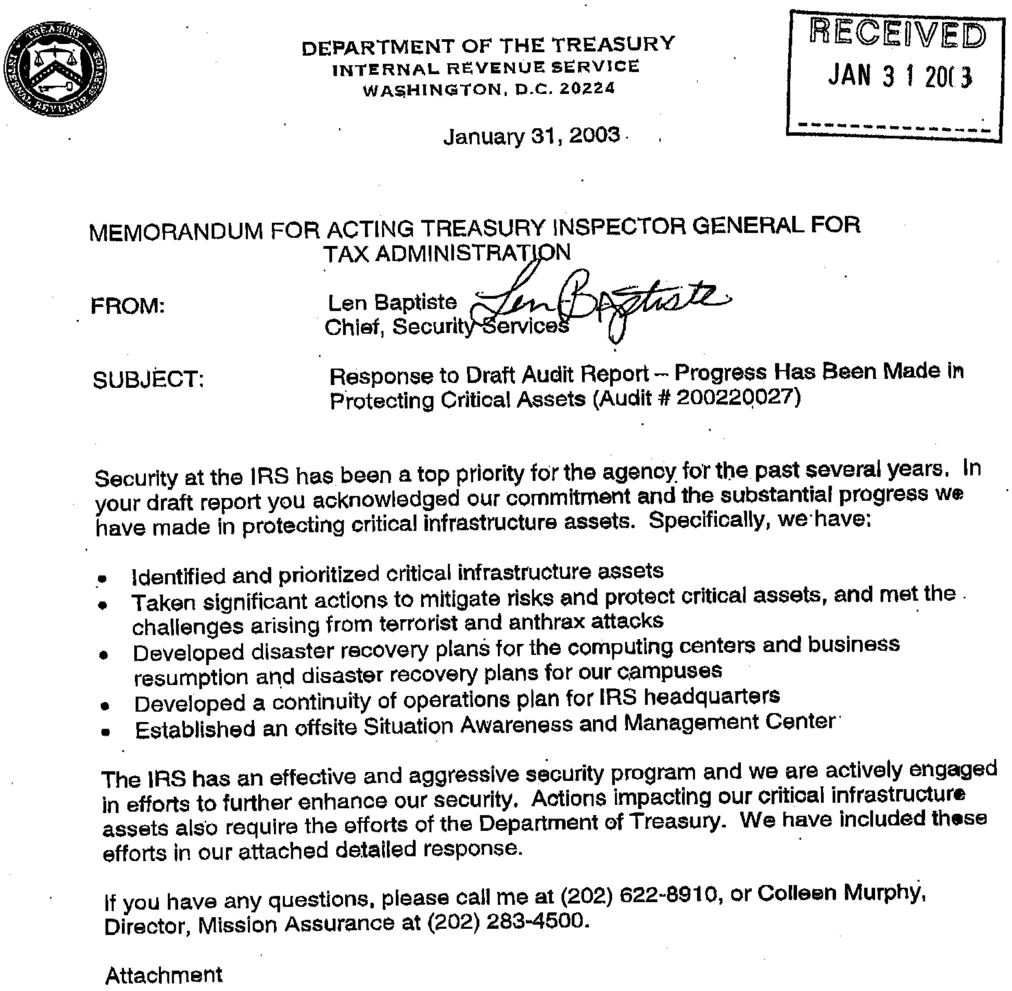
Appendix III

Report Distribution List

Acting Commissioner N:C
Chief, Security Services M:S
Chief Counsel CC
National Taxpayer Advocate TA
Director, Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O
Office of Management Controls N:CFO:F:M
Audit Liaisons:
    Deputy Commissioner for Modernization & Chief Information Officer M
    Chief, Security Services M:S

Appendix IV

Management's Response to the Draft Report



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

RECEIVED
JAN 3 1 2003

January 31, 2003

MEMORANDUM FOR ACTING TREASURY INSPECTOR GENERAL FOR
TAX ADMINISTRATION

FROM: Len Baptiste Len Baptiste
Chief, Security Services

SUBJECT: Response to Draft Audit Report – Progress Has Been Made in Protecting Critical Assets (Audit # 200220027)

Security at the IRS has been a top priority for the agency for the past several years. In your draft report you acknowledged our commitment and the substantial progress we have made in protecting critical infrastructure assets. Specifically, we have:

- Identified and prioritized critical infrastructure assets
- Taken significant actions to mitigate risks and protect critical assets, and met the challenges arising from terrorist and anthrax attacks
- Developed disaster recovery plans for the computing centers and business resumption and disaster recovery plans for our campuses
- Developed a continuity of operations plan for IRS headquarters
- Established an offsite Situation Awareness and Management Center

The IRS has an effective and aggressive security program and we are actively engaged in efforts to further enhance our security. Actions impacting our critical infrastructure assets also require the efforts of the Department of Treasury. We have included these efforts in our attached detailed response.

If you have any questions, please call me at (202) 622-8910, or Colleen Murphy, Director, Mission Assurance at (202) 283-4500.

Attachment

TIGTA Report Entitled: Progress Has Been Made in Protecting Critical Assets (Audit #200220027)

RECOMMENDATION # 1
Identify the critical data that are shared with other federal and state entities and implement specific procedures to protect those data. Also, the CIAO should identify the critical data that are received by the IRS and implement specific procedures to protect those data.

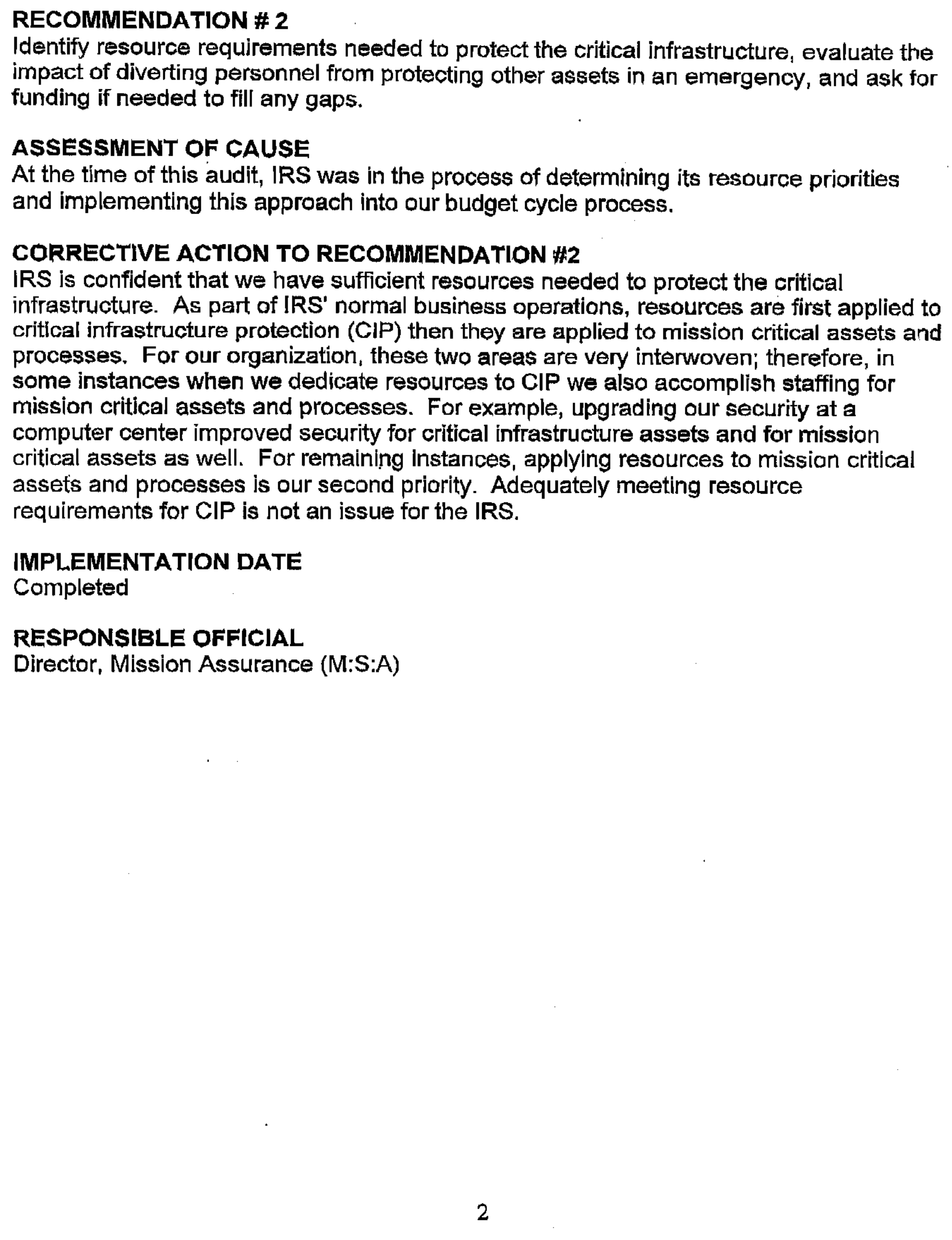
ASSESSMENT OF CAUSE
The Department of Treasury is taking action to address this recommendation. Specifically, the Department of Treasury is leading the effort to identify critical data that are shared by Treasury entities with other federal and state entities. During the fourth quarter of calendar year 2002, a pilot test conducted by Treasury, and its Financial Crimes Enforcement Network (FinCEN) provided the methodology that Treasury and its contractor will use to perform an interdependency analysis. This analysis will identify the shared critical data.

BACKGROUND
In response to Presidential Decision Directive 63 and Critical Infrastructure Protection, the federal government implemented an approach called Project Matrix. A component part of Project Matrix is to identify critical data that are shared with other entities. Specifically, Step 2 of Project Matrix entails conducting a functional analysis on each critical asset to identify public and private sector interdependencies and possible points of failure. This Interdependency Analysis was recently commenced under the direction of the Department of Treasury. IRS has eight critical assets scheduled by Treasury to undergo Interdependency Analysis during calendar year 2003. This analysis will identify the shared critical data.

CORRECTIVE ACTION TO RECOMMENDATION #1
Based on the results of Treasury's Interdependency Analysis, IRS will take action to determine the appropriate level of security needed to adequately protect all critical data—shared or received. IRS will review and mitigate existing vulnerabilities to ensure the appropriate level of security. These efforts will be conducted in accordance with our existing standards to protect critical assets.

IMPLEMENTATION DATE
October 1, 2004

RESPONSIBLE OFFICIAL
Director, Mission Assurance (M:S:A)



RECOMMENDATION # 2
Identify resource requirements needed to protect the critical infrastructure, evaluate the impact of diverting personnel from protecting other assets in an emergency, and ask for funding if needed to fill any gaps.

ASSESSMENT OF CAUSE
At the time of this audit, IRS was in the process of determining its resource priorities and implementing this approach into our budget cycle process.

CORRECTIVE ACTION TO RECOMMENDATION #2
IRS is confident that we have sufficient resources needed to protect the critical infrastructure. As part of IRS' normal business operations, resources are first applied to critical infrastructure protection (CIP) then they are applied to mission critical assets and processes. For our organization, these two areas are very interwoven; therefore, in some instances when we dedicate resources to CIP we also accomplish staffing for mission critical assets and processes. For example, upgrading our security at a computer center improved security for critical infrastructure assets and for mission critical assets as well. For remaining instances, applying resources to mission critical assets and processes is our second priority. Adequately meeting resource requirements for CIP is not an issue for the IRS.

IMPLEMENTATION DATE
Completed

RESPONSIBLE OFFICIAL
Director, Mission Assurance (M:S:A)